DETAILED ACTION

Continued Examination Under 37 CFR 1.114

A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 6/18/2009 has been entered.

Examiner's Amendment

An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee.

Authorization for this Examiner's Amendment was given in a telephone interview with James J. Kulbaski (Reg. No. 34,648) on 17 July 2009.

This application has been amended as follows:

IN THE CLAIMS

Cancel claim 1 – 15 and 25.

Replace claim 16 and 28 as follows.

Claim 16:

A denial-of-service attack detecting system for detecting a denial-of-service attack on a communication device, the denial-of-service attack detecting system comprising:

a monitoring device that monitors each packet transmitted to the communication device and includes a traffic abnormality detecting unit that detects traffic abnormality information indicating an abnormality of traffic based on packets transmitted to the communication device;

a performance measuring device that measures response performance of the communication device based on a performance abnormality detection condition including a response time from transmission of a response request message to the communication device, to reception of a response message corresponding to the response request message, the performance measuring device being separate from and connected with the communication device and the monitoring device through a network, the performance measuring device including a performance abnormality detecting unit that detects performance abnormality information indicating an abnormality of throughput of the communication device; and

an attack determining device that is connected to and performs communication with the monitoring device and the performance measuring device,

the attack determining device including an effects determining unit that determines whether the communication device has received the denial-of-service attack, using both the traffic abnormality information and the performance abnormality information, and

the effects determining unit determining that the communication device has received the denial-of-service attack, when it is determined that one of the traffic abnormality information and the performance abnormality information causes an occurrence of one of the traffic abnormality information and the performance abnormality information based on an abnormality occurrence time included in the traffic abnormality information and the performance abnormality information.

Claim 28:

A method of detecting a denial-of-service attack on a communication device by using a monitoring device that monitors each packet transmitted to the communication device, a performance measuring device that measures response performance of the communication device based on a performance abnormality detection condition including a response time from transmission of a response request message to the communication device, to reception of a response message corresponding to the response request message, ~~and the performance measuring device being separate from the communication device and the monitoring device.~~ and an attack determining device that is connected to and performs communication with the monitoring device and the performance measuring device, the method comprising:

detecting a traffic abnormality using the monitoring device to detect traffic abnormality information indicating an abnormality of traffic based on packets transmitted to the communication device;

detecting performance abnormality information using the performance measuring device to detect performance abnormality information indicating an abnormality of throughput of the communication device, wherein the performance measuring device being separate from and connected with the communication device and the monitoring device through a network; and

determining effects using the attack determining device to determine whether the communication device has received the denial-of-service attack, using both the traffic abnormality information and the performance abnormality information, the determining including determining that the communication device has received the denial-of-service attack, when it is determined that one of the traffic abnormality information and the performance abnormality information causes an occurrence of one of the traffic abnormality information and the performance abnormality information based on an abnormality occurrence time included in the traffic abnormality information and the performance abnormality information .

Allowable Subject Matter

Claims 16 – 24 and 26 – 30 are allowed.

The following is an examiner's statement of reasons for allowance:

The above mentioned claims are allowable over prior arts because the CPA (Cited Prior Art) of record fails to teach or render obvious the claimed limitations in combination with the specific added limitations recited in claims 16 and 28 (& associated dependent claims).

The present invention is directed to a method for detecting a denial-of-service attack on a communication device by using a monitoring device that monitors each packet transmitted to the communication device, a performance measuring device that measures response performance of the communication device based on a performance abnormality detection condition including a response time from transmission of a response request message to the communication device, to reception of a response message corresponding to the response request message, and an attack determining device that is connected to and performs communication with the monitoring device and the performance measuring device. No singular art disclosing, nor motivation to combine has been found to anticipate or render obvious the claimed invention of detecting a traffic abnormality using the monitoring device to detect traffic abnormality information indicating an abnormality of traffic based on packets transmitted to the communication device; detecting performance abnormality information using the performance measuring device to detect performance abnormality information indicating an abnormality of throughput of the communication device, wherein the performance measuring device being separate from and connected with the communication device and the monitoring device through a network; and determining effects using the attack determining device to determine whether the communication device has received the denial-of-service attack, using both the traffic abnormality information and the performance abnormality information, the determining including determining that the communication device has received the denial-of-service attack, when it is determined that one of the traffic abnormality information and the performance abnormality information causes an occurrence of one of the traffic abnormality information and the performance abnormality information based on an abnormality occurrence time included in the traffic abnormality information and the performance abnormality information.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to LONGBIT CHAI whose telephone number is (571)272-3788. The examiner can normally be reached on Monday-Friday 9:00am-5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, William R. Korzuch can be reached on (571) 272-7589. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Longbit Chai/

Primary Patent Examiner
Art Unit 2431
7/27/2009